RECEIVED
CENTRAL FAX CENTER
JAN 09 2007

AMENDMENTS TO THE CLAIMS

• Please amend the claims as follows:

1. (cancelled)

2. (previously presented) The method of claim 42, wherein applying the transformation generates encrypted data that is indistinguishable from Gaussian white noise.

3. (previously presented) The method of claim 42, wherein applying the transformation comprises normalizing the measurements.

4. (previously presented): The method of claim 3 wherein the normalizing step comprises centering and scale-transforming the measurements so that the mean is zero and the standard deviation is 1.

5. (previously presented) The method of claim 42, wherein applying the transformation comprises permuting the measurements.

6. (original): The method of claim 5 wherein permuting comprises employing an item of secret information.

7. (original): The method of claim 6 wherein permuting comprises employing a passcode.

8. (original): The method of claim 7 wherein permuting additionally comprises employing the results of a hash function of the passcode.

9. (previously presented) The method of claim 42, wherein applying the transformation comprises employing a linear transformation.

PAGE 3/14 * RCVD AT 1/9/2007 4:28:01 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/13 * DNIS:2738300 * CSID:+15058442829 * DURATION (mm-ss):02-46

10. (previously presented) The method of claim 9 wherein employing a linear transformation comprises employing a *n x m* linear transformation matrix, **W**, with orthonormal columns, where $n \leq m$.

11. (original): The method of claim 10 wherein employing a linear transformation comprises employing a normalized Hadamard matrix.

12. (original): The method of claim 10 wherein employing a linear transformation comprises employing a normalized matrix comprising Fourier coefficients with a cosine / sine basis.

13. (previously presented): The method of claim 9 wherein employing a linear transformation comprises permuting the linearly transformed data.

14. (original): The method of claim 13 wherein permuting the linearly transformed data comprises employing an item of secret information.

15. (original): The method of claim 14 wherein permuting the linearly transformed data comprises employing a passcode.

16. (original): The method of claim 15 wherein permuting the linearly transformed data additionally comprises employing the results of a hash function of the passcode.

17. (previously presented) The method of claim 42, wherein the measurements comprise biometric data.

18. (original): The method of claim 17 wherein the measurements comprise measurements selected from the group consisting of fingerprints, retinal scans, facial scans, hand geometry, spectral data, and voice data.

19. (previously presented) The method of claim 17, additionally comprising the step of placing reference biometric data on a smart card to be carried by an individual from whom the biometric data was taken.

20. (previously presented) The method of claim 42, wherein the measurements comprise spectral data.

21. (original): The method of claim 20 wherein the measurements comprise weapons spectra.

22. (previously presented) The method of claim 42, additionally comprising the step of adding pseudo-dimensions to the measurements to enhance concealment.

23-41. (cancelled)

42. (currently amended) A method of authenticating an item, the method comprising:

a) acquiring an unencrypted reference signal, $\boldsymbol{Y_{ref}}$, of an item; where $\boldsymbol{Y_{ref}}$ is an n-dimensional row vector $\{Y_1(ref), Y_2(ref), \ldots, Y_n(ref)\}$ of unencrypted reference measurements subject to measurement error;

b) applying a transformation to the unencrypted reference signal, $\boldsymbol{Y_{ref}}$, to generate an encrypted reference signal, $\boldsymbol{U_{ref}}$ of the item; where $\boldsymbol{U_{ref}}$ is an n-dimensional row vector $\{U_1(ref), U_2(ref), \ldots, U_n(ref)\}$ of encrypted reference measurements;

c) acquiring an unencrypted new signal, $\boldsymbol{Y_{new}}$, of the item, where $\boldsymbol{Y_{new}}$ is an n-dimensional row vector $\{Y_1(new), Y_2(new), \ldots, Y_n(new)\}$ of unencrypted new measurements subject to measurement error;

d) applying the transformation to the unencrypted new signal, $\boldsymbol{Y_{new}}$, to generate an encrypted new signal, $\boldsymbol{U_{new}}$, of the item; where $\boldsymbol{U_{new}}$ is an *n*-dimensional row vector $\{U_1(new), U_2(new), \ldots, U_n(new)\}$ of encrypted new measurements;

e) calculating an unencrypted Euclidean distance metric, $\boldsymbol{E}$, between the unencrypted new and reference signals, $\boldsymbol{Y_{new}}$ *and* $\boldsymbol{Y_{ref}}$;

f) calculating an encrypted Euclidean distance metric, D, between the encrypted new and reference measurements, $\boldsymbol{U_{new}}$ *and* $\boldsymbol{U_{ref}}$;

g) comparing the encrypted Euclidean distance metric, D, to a critical value, D_{crit}, ~~and~~;

[[e)]] <u>h)</u> if $D < D_{crit}$, then deciding that the item is authentic; and

<u>i) providing the result of the decision made in step h) to an authenticator or inspector, thereby allowing the authenticator or inspector to decide if the item is authentic;</u>

wherein the transformation has the property that the unencrypted Euclidean distance metric, E, is equal to the encrypted Euclidean distance metric, D.

43. (currently amended) The method of claim 42, wherein:

$$\cancel{E = \sum_{j=1}^{n}\left(Y_j(\text{new}) - Y_j(reference)\right)^2;}$$

$$E = \sum_{j=1}^{n}\left(Y_j(\text{new}) - Y_j(ref)\right)^2$$

and

$$\cancel{D = \sum_{j=1}^{m}\left(U_j(\text{new}) - U_j(reference)\right)^2,}$$

$$D = \sum_{j=1}^{m}\left(U_j(\text{new}) - U_j(ref)\right)^2$$

wherein $m \leq n$.

44. (currently amended) The method of claim 42, wherein:

$$\cancel{E = \sum_{j=1}^{n} \frac{\left(Y_j(\text{new}) - Y_j(\textit{reference})\right)^2}{Y_j};}$$

$$E = \sum_{j=1}^{n} \frac{\left(Y_j(\text{new}) - Y_j(\text{r}ef)\right)^2}{Y_j}$$

and

$$\cancel{D = \sum_{j=1}^{m} \frac{\left(U_j(\text{new}) - U_j(\textit{reference})\right)^2}{Y_j};}$$

$$D = \sum_{j=1}^{m} \frac{\left(U_j(\text{new}) - U_j(\text{r}ef)\right)^2}{Y_j}$$

wherein $m \leq n$; and the denominator can be either $Y_j(new)$ or ~~$Y_j(reference)$~~ <u>$Y_j(ref)$.</u>

45. (currently amended) The method of claim 42, wherein:

$$\cancel{E = \sum_{j=1}^{n}\left(\sqrt{Y_j}(\text{new}) - \sqrt{Y_j}(\mathit{reference})\right)^2;}$$

$$E = \sum_{j=1}^{n}\left(\sqrt{Y_j}(\text{new}) - \sqrt{Y_j}(\mathit{ref})\right)^2$$

and

$$\cancel{D = \sum_{j=1}^{m}\left(\sqrt{U_j}(\text{new}) - \sqrt{U_j}(\mathit{reference})\right)^2;}$$

$$D = \sum_{j=1}^{m}\left(\sqrt{U_j}(\text{new}) - \sqrt{U_j}(\text{ref})\right)^2$$

wherein $m \leq n$.

46. (previously presented) The method of claim 10, wherein the elements, w_{ij}, of the transformation matrix, **W**, have the following properties:

$$\sum_{i=1}^{n} w_{ij}^2 = 1, \forall_j \quad ;$$

$$w_{i1} = \frac{1}{\sqrt{n}}, \forall_i \quad ; \text{and}$$

$$\sum_{i=1}^{n} w_{ij} = 0, \forall_{j>1} \text{ with } w_{i1} = K, \ \forall_{i}.$$

47. (previously presented) The method of claim 42, wherein applying the transformation to the unencrypted signal, **Y**, comprises:

$$Y \rightarrow Y_{\pi} \rightarrow Y_{\pi} \cdot W \rightarrow (Y_{\pi} \cdot W)_{\sigma}$$

wherein:

π is a *permutation* of the integers from 1:*n* that is unique to a particular verification class;

W is an *n* x *m* transformation matrix with orthonormal columns that transforms the vector, **Y**, of measurements to $m \le n$ latent variables; and

σ is a *permutation* of the integers from 1:*m* that is unique to the particular verification class; and

wherein the verification class comprises one or more physical units, items, or individuals.